

## UNITED STATES DISTRICT COURT

for the  
District of Arizona

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 Blue 2018 Hyundai Sonata, (VIN)  
 5NPE34AF0JH652452, bearing Arizona  
 license plate BXA8CBA

)  
 )  
 ) Case No. 21-8298MB  
 )  
 )  
 )

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search  
 of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Arizona

(identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated by reference

The person or property to be searched, described above, is believed to conceal (identify the person or describe the  
 property to be seized):

See Attachment B, incorporated by reference

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or  
 property.

**YOU ARE COMMANDED** to execute this warrant on or before

December 1, 2021

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.

☐ at any time in the day or night as I find reasonable cause has been  
 established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property  
 taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the  
 place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an  
 inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge  
 on duty in the District of Arizona \_\_\_\_\_.

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay  
 of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be  
 searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued:

Nov. 17, 2021 @ 3:25 AM

91305

Judge's signature

City and state: Phoenix Arizona

JOHN Z. BOYLE, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

A Blue 2018 Hyundai Sonata, Vehicle Identification Number (VIN) 5NPE34AF0JH652452, bearing Arizona license plate BXA8CBA, currently in the custody of ATF - Phoenix.

**ATTACHMENT B**

**PROPERTY TO BE SEIZED**

Agents are authorized to search for evidence, contraband, fruits, or instrumentalities of violations of Title 18, U.S.C. § 924(a)(1)(A), knowingly making any false statement with respect to the information required by federal law to be kept by the holder of a Federal Firearms License (FFL); and, as further described in the affidavit of probable cause including:

1. Any firearms including firearms parts, frames, receivers, accessories, magazines, cases, boxes;
2. Any ammunition and components including, bullets, brass, casings, boxes, and cases;
3. US Currency;
4. Concealed Weapons Permit.
5. The following records relating to the violations of 18 U.S.C. § 922(a)(1)(A) (Engaging in the business of dealing, importing, manufacturing firearms without a license) and 18 U.S.C. § 924(d) (Sell or otherwise dispose of firearms or ammunition to any person who is prohibited under Title 18 USC §922(g)):
  - a. Records, documents, notes, receipts, ledgers, invoices, indicia, or photographs showing the acquisition or sale of any firearms and firearm parts;
  - b. Receipts, bank account records, buyer or seller lists, money transfer records, agreements for storage facilities, records of mail service, ledgers, and notebooks showing the acquisition and/or disposition of firearms and firearm parts;

- c. Books, records, receipts, notes, ledgers, personal checks and other papers relating to the transportation, ordering, and purchase of firearms, firearm accessories, or ammunition;
  - d. Ledgers, customer lists, contact lists, inventory lists, vendor lists, or any notes containing the individual names of such persons, telephone numbers or addresses of such persons; and,
  - e. Bank documents and records, financial documents and records, and any records and documents relating to any bank or financial transactions, including: correspondence, signature cards and applications for all credit card accounts, investment accounts, and retirement accounts; copies of monthly, quarterly, yearly or periodic account statements; pre-paid credit/debit cards; money wrappers; copies of check journals, check ledgers, checkbooks, check registers, deposit tickets, deposit items, credit memos, debit memos, canceled checks, loan applications, financial statements, mortgage or promissory notes; copies of loan ledger accounts; copies of annual loan statements; application for bank drafts, cashier's checks, and foreign drafts; and records relating to employment, wages earned and paid, business income earned, and other compensation records.
- 6. Records indicating occupancy, residency, rental or ownership of the search location, including utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, and keys;
  - 7. Any and all records pertaining to the rental of self-storage units and post office boxes or mailboxes;
  - 8. Electronic equipment, including cellular telephones, computers, disks, thumb drives, and any media storage device, GPS devices and their memory, and related manuals used to generate, transfer, count, record or store the information described in this attachment. For any computer or electronic storage medium whose seizure

is otherwise authorized by this warrant, and any computer or electronic storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, the “Electronic Storage Device”), this warrant also authorizes the seizure of the following:

- a. Evidence of who used, owned, or controlled the Electronic Storage Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, and browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Call details including call history, duration of calls, text messages, and text message history;
- c. Electronic correspondence and communications stored on, or accessed through, the Electronic Storage Device relating to the procurement of export-controlled items, to include e-mails and attached files, text messages, any Short Message Service messages (SMS), Instant Messages (IM), Multimedia Message Service messages, or similar text or electronic messages made through additional applications from which communication can be made, and instant messaging logs;
- d. Contact lists stored on or accessed through the Electronic Storage Device, to include telephone and e-mail contact names, telephone numbers, addresses, and e-mail addresses;
- e. Evidence of software that would allow others to control the Electronic Storage Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms

that the user entered into any Internet search engine, and records of user-typed web addresses;

g. Evidence indicating how and when the Electronic Storage Device was accessed or used to determine the chronological context of Electronic Storage Device access, use, and events relating to crime under investigation and to the user of the Electronic Storage Device;

h. Evidence of the attachment to the Electronic Storage Device of other storage devices or similar containers for electronic evidence;

i. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Electronic Storage Device;

j. Evidence of the times the Electronic Storage Device was used;

k. Passwords, encryption keys, and other access devices that may be necessary to access the Electronic Storage Device;

l. Documentation and manuals that may be necessary to access the Electronic Storage Device or conduct an examination of the Electronic Storage Device;

m. Any records of or information about Internet Protocol addresses used by the Electronic Storage Device;

n. Contextual information necessary to understand the evidence described in this attachment; and,

o. Any peripheral equipment used to facilitate the transmission, creation, display, encoding or storage of records, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners.

9. Items used for identification, including identification cards under fictitious names, and any other type of false identifying documents.

## UNITED STATES DISTRICT COURT

for the  
District of Arizona

In the Matter of the Search of  
*(Briefly describe the property to be searched  
 or identify the person by name and address)*  
 Blue 2018 Hyundai Sonata, (VIN)  
 5NPE34AF0JH652452, bearing Arizona  
 license plate BXA8CBA

Case No.

21-8298 MB

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See attachment A, incorporated by reference.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Arizona \_\_\_\_\_, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 18 U.S.C. § 924(a)(1)(A)	Knowingly making any false statement with respect to the information required by federal law to be kept by the holder of a Federal Firearms License (FFL)

The application is based on these facts:  
 See attached Affidavit, incorporated by reference.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Brett Day  
 Reviewed by Brett A. Day, AUSA

[Signature]  
 Applicant's signature

Katherine A Rottman, Special Agent, ATF  
 Printed name and title

Sworn to and signed electronically.

Date: 11/17/2021

[Signature]  
 Judge's signature

City and state: Phoenix, Arizona

JOHN Z. BOYLE, U.S. Magistrate Judge  
 Printed name and title

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

A Blue 2018 Hyundai Sonata, Vehicle Identification Number (VIN) 5NPE34AF0JH652452, bearing Arizona license plate BXA8CBA, currently in the custody of ATF - Phoenix.

**ATTACHMENT B**

**PROPERTY TO BE SEIZED**

Agents are authorized to search for evidence, contraband, fruits, or instrumentalities of violations of Title 18, U.S.C. § 924(a)(1)(A), knowingly making any false statement with respect to the information required by federal law to be kept by the holder of a Federal Firearms License (FFL); and, as further described in the affidavit of probable cause including:

1. Any firearms including firearms parts, frames, receivers, accessories, magazines, cases, boxes;
2. Any ammunition and components including, bullets, brass, casings, boxes, and cases;
3. US Currency;
4. Concealed Weapons Permit.
5. The following records relating to the violations of 18 U.S.C. § 922(a)(1)(A) (Engaging in the business of dealing, importing, manufacturing firearms without a license) and 18 U.S.C. § 924(d) (Sell or otherwise dispose of firearms or ammunition to any person who is prohibited under Title 18 USC §922(g)):
  - a. Records, documents, notes, receipts, ledgers, invoices, indicia, or photographs showing the acquisition or sale of any firearms and firearm parts;
  - b. Receipts, bank account records, buyer or seller lists, money transfer records, agreements for storage facilities, records of mail service, ledgers, and notebooks showing the acquisition and/or disposition of firearms and firearm parts;

- c. Books, records, receipts, notes, ledgers, personal checks and other papers relating to the transportation, ordering, and purchase of firearms, firearm accessories, or ammunition;
  - d. Ledgers, customer lists, contact lists, inventory lists, vendor lists, or any notes containing the individual names of such persons, telephone numbers or addresses of such persons; and,
  - e. Bank documents and records, financial documents and records, and any records and documents relating to any bank or financial transactions, including: correspondence, signature cards and applications for all credit card accounts, investment accounts, and retirement accounts; copies of monthly, quarterly, yearly or periodic account statements; pre-paid credit/debit cards; money wrappers; copies of check journals, check ledgers, checkbooks, check registers, deposit tickets, deposit items, credit memos, debit memos, canceled checks, loan applications, financial statements, mortgage or promissory notes; copies of loan ledger accounts; copies of annual loan statements; application for bank drafts, cashier's checks, and foreign drafts; and records relating to employment, wages earned and paid, business income earned, and other compensation records.
- 6. Records indicating occupancy, residency, rental or ownership of the search location, including utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, and keys;
  - 7. Any and all records pertaining to the rental of self-storage units and post office boxes or mailboxes;
  - 8. Electronic equipment, including cellular telephones, computers, disks, thumb drives, and any media storage device, GPS devices and their memory, and related manuals used to generate, transfer, count, record or store the information described in this attachment. For any computer or electronic storage medium whose seizure

is otherwise authorized by this warrant, and any computer or electronic storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, the “Electronic Storage Device”), this warrant also authorizes the seizure of the following:

- a. Evidence of who used, owned, or controlled the Electronic Storage Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, and browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Call details including call history, duration of calls, text messages, and text message history;
- c. Electronic correspondence and communications stored on, or accessed through, the Electronic Storage Device relating to the procurement of export-controlled items, to include e-mails and attached files, text messages, any Short Message Service messages (SMS), Instant Messages (IM), Multimedia Message Service messages, or similar text or electronic messages made through additional applications from which communication can be made, and instant messaging logs;
- d. Contact lists stored on or accessed through the Electronic Storage Device, to include telephone and e-mail contact names, telephone numbers, addresses, and e-mail addresses;
- e. Evidence of software that would allow others to control the Electronic Storage Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- f. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms

that the user entered into any Internet search engine, and records of user-typed web addresses;

g. Evidence indicating how and when the Electronic Storage Device was accessed or used to determine the chronological context of Electronic Storage Device access, use, and events relating to crime under investigation and to the user of the Electronic Storage Device;

h. Evidence of the attachment to the Electronic Storage Device of other storage devices or similar containers for electronic evidence;

i. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Electronic Storage Device;

j. Evidence of the times the Electronic Storage Device was used;

k. Passwords, encryption keys, and other access devices that may be necessary to access the Electronic Storage Device;

l. Documentation and manuals that may be necessary to access the Electronic Storage Device or conduct an examination of the Electronic Storage Device;

m. Any records of or information about Internet Protocol addresses used by the Electronic Storage Device;

n. Contextual information necessary to understand the evidence described in this attachment; and,

o. Any peripheral equipment used to facilitate the transmission, creation, display, encoding or storage of records, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners.

9. Items used for identification, including identification cards under fictitious names, and any other type of false identifying documents.

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Katherine A Rottman being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. This affidavit is submitted in support of an application for a warrant to search the following property, which is further described in Attachment A, for evidence of a violation of Title 18, U.S.C. § 924(a)(1)(A), knowingly making any false statement with respect to the information required by federal law to be kept by the holder of a Federal Firearms License (FFL): a 2018 Hyundai Sonata, Vehicle Identification Number (VIN) 5NPE34AF0JH652452, bearing Arizona license plate BXA8CBA (hereinafter **SUBJECT VEHICLE**), currently in the custody of ATF - Phoenix.

2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF) and have been since June 2020. I am graduate of the Federal Law Enforcement Training Center (FLETC) Criminal Investigator Training Program (CITP) and a graduate of the ATF National Academy Special Agent Basic Training (SABT) programs in Glynco, Georgia. I am empowered by law to conduct investigations of and make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. My training in law enforcement includes agency specific training in all aspects of conducting federal criminal investigations, including the planning, preparation, and execution of search warrants. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, U.S.C. § 2510(7), authorized to conduct investigations into alleged violations of federal law.

4. Through my training and experience, I know that it is a violation of federal law for any person who knowingly makes a false statement or representation with respect to the information required by federal law to be kept in the records of an FFL according to Title 18, U.S.C., U.S.C. § 924(a)(1)(A).

5. This affidavit is intended to show that there is sufficient probable cause for the requested search warrant and does not purport to set forth all my knowledge of or investigation into this matter. The statements set forth in this affidavit are based upon my investigation to date, my experience, my training, and other reliable sources of information relative to this investigation.

#### **PROPERTY TO BE SEARCHED**

6. The property to be searched is described in Attachment A, incorporated herein by reference.

#### **ITEMS TO BE SEIZED**

7. The items to be seized are described in Attachment B, incorporated herein by reference.

#### **PROBABLE CAUSE**

##### **Introduction**

5. As of October 2021, ATF has been investigating the activities of HUERTA regarding his violations of Title 18, U.S.C. § 924(a)(1)(A), knowingly making a false statement or representation with respect to the records required by federal law to be kept by an FFL.

6. On November 3, 2021, Your Affiant received information that HUERTA had purchased a total of 35 firearms since June 22, 2021. Since HUERTA's 21<sup>st</sup> birthday in August of this year, he has only purchased pistols, while prior to his 21<sup>st</sup> birthday, HUERTA had only purchased rifles. Per the GCA, individuals can only legally purchase rifles at the age of 18 and can legally purchase handguns at the age of 21. Since September 30, 2021, HUERTA has purchased total of 24 total Glock 19x 9mm firearms.

7. Two of the firearms HUERTA purchased have been recovered at a crime scene in Phoenix, Arizona. On October 24, 2021, Phoenix Police Department (PPD) responded to reports of gunshots being fired at a large house party located at 78<sup>th</sup> Ave, Phoenix, Arizona. While PPD was at the scene, they heard several additional gunshots. The reporting party notified PPD that a red Ford truck bearing AZ plate A3A23E was responsible for the gunshots. PPD located the red Ford truck bearing AZ plate A3A23E and recovered three firearms. Two of the recovered firearms were purchased by HUERTA 6-days, and 10-days, prior to their recovery, respectively.

8. PPD identified two of the six occupants inside the red Ford truck as juvenile I.G. (xx/xx/2005) and adult D.V. (xx/xx/2001). D.V. admitted to ownership of the three recovered firearms. Both I.G. and D.V. are currently under investigation by PPD for other drive-by shootings at house parties in the Phoenix area.

9. As part of that separate state investigation into the drive-by shootings, ATF Task Force Officer (TFO) George Fulton obtained a state search warrant for I.G.'s Snapchat account. From I.G.'s snapchat account, TFO Fulton observed that I.G. is

advertising firearms for sale, and observed photos of I.G. holding firearms of a similar make and model to the firearms that HUERTA has recently purchased.

10. In one photo, TFO Fulton observed on I.G.'s Snapchat account a photo of a CZ Scorpion pistol being offered for sale. In the photo, the serial number is visible. The serial number of the CZ Scorpion pistol in the photo matches the serial number of a CZ Scorpion purchased by HUERTA from FFL Ammo AZ on October 6, 2021.

11. On October 26, 2021, TFO Fulton visited Ammo AZ regarding HUERTA's purchase of the CZ Scorpion pistol. Employees with Ammo AZ informed TFO Fulton that they observed HUERTA get in and out of a blue Hyundai bearing AZ plate BXA8CBA (Subject Vehicle) when purchasing the CZ Scorpion pistol.

12. Additionally, 4 firearms by HUERTA were recovered by Arizona Department of Safety on or about November 11, 2021. All four firearms were purchased by HUERTA on October 22<sup>nd</sup>, 2021.

13. On October 28, 2021, Buckeye Police Department (BPD) officers conducted surveillance at 210 E Jackson Ave., Unit 1, Buckeye, Arizona, 85326, the registered address of the **SUBJECT VEHICLE**. During the surveillance, BPD observed the **SUBJECT VEHICLE** at the residence. Additionally, 210 E Jackson Ave., Unit 1, Buckeye, Arizona, 85326, is HUERTA's registered address with Arizona MVD, as well as the address HUERTA is providing on all ATF Form 4473s as his residential address..

14. On November 8, 2021, HUERTA purchased a total of five Glock 19x 9mm pistols at various FFLs in the Phoenix area. One of those purchases occurred at FFL

Glockmeister, located in Phoenix, Arizona. Glockmeister notified Your Affiant that they observed surveillance footage from HUERTA's purchase of the firearms and informed that HUERTA can be observed getting into a blue Hyundai Sonata (**SUBJECT VEHICLE**) following the purchase. Glockmeister provided the below still photos captured from the surveillance footage.



15. On November 10, 2021, at approximately 3:29 pm. Your Affiant received a federal warrant for GPS tracking for the **SUBJECT VEHICLE**. Your Affiant was able to determine the following, based on the GPS tracker:

16. On November 12, 2021, HUERTA arrived in the **SUBJECT VEHICLE** at Scottsdale Gun Club at 11:06 am. HUERTA purchased 1 Micro Draco pistol bearing serial number 21PMD-25895, and one FN Five Seven pistol bearing 386412643. After his purchase, HUERTA visited the parking lot of another Federal Firearms Licensee, Tactical Studio, which is located at 5023 W Olive Ave. After visiting Tactical Studio, HUERTA stops at the Fry's located at 5116 W Olive Ave, then proceeds to drive the **SUBJECT VEHICLE** to his residence at 210 E Jackson Ave Unit 1 Buckeye, AZ 85326.

17. On November 16, 2021, HUERTA leaves his residence at 8:09 am in the **SUBJECT VEHICLE**. HUERTA drove to Harbor Freight, located at 3146 E Thomas Road. HUERTA then drove to FFL Bear Arms, located at 10321 N Scottsdale Rd Scottsdale, AZ 85253, and purchased a FN pistol bearing serial number 386413559. Surveillance units observed HUERTA leave Bear Arms with a gun box and drive to 1600 E Camelback Road, where he met a Hispanic male in a red Ford F150 pickup truck, bearing AZ plate A3A23E. The Ford F150 pickup truck, bearing AZ plate A3A23E is the same pickup truck that was the subject of the drive-by shooting that occurred on October 24, 2021.

18. Surveillance units observed HUERTA hand the gun box off to the Hispanic male in the driver's seat. Surveillance units observed the Hispanic male in the red Ford F150 drive across the street and hand off the gun box to Jesus CAVARES. Surveillance units developed probable cause for a traffic stop of CAVARES. Upon conducting the traffic stop, CAVARES pulled to the side of the road and bailed from the vehicle. Upon bailing from the vehicle, the FN pistol bearing serial number 386413559 fell out of CAVARES's vehicle as CAVARES attempted to flee from the vehicle stop. CAVARES was subsequently arrested.

19. In a search of the vehicle, units observed a Micro Draco pistol bearing serial number 21PMD-25895, the same as the Micro Draco pistol purchased by HUERTA on November 12, 2021 from Scottsdale Gun Club and transported in the **SUBJECT VEHICLE** to his residence. In addition to the two pistols recovered which were previously purchased by HUERTA, law enforcement also recovered approximately 12,000 fentanyl pills in CAVARES' vehicle.

20. Following the traffic stop and subsequent arrest of CAVARES, surveillance units continued to surveil HUERTA. HUERTA was next observed driving to FFL One Stop Firearms, located at 7602 E Main St Mesa, AZ 85207. Surveillance units observed HUERTA leave the FFL with a blue gun box. HUERTA placed the blue gun box into his vehicle and left the FFL. Believing that HUERTA would again transfer the firearm he purchased to another individual, units initiated a traffic stop, and placed HUERTA under arrest for his violations of Title 18 United States Code, Section 924(a)(1)(a). The

**SUBJECT VEHICLE** was impounded and HUERTA was transported to Phoenix Police Headquarters.

**TRAINING AND EXPERIENCE – DIGITAL DEVICES/MEDIA**

21. Through my training and experience as an ATF SA, I have learned that many people keep records of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. It has been my experience that unlicensed dealers of firearms who purchase firearms illegally will keep the contact information of the individual to whom he or she sells firearms for future sales and/or sales referrals from established customers. I know that much correspondence is via digital devices. I know that much correspondence between persons buying and selling firearms often occurs by e-mail or text message sent to and from digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price.

22. Therefore, based on my experience, I believe that it is probable that digital devices may contain text messages or e-mails between HUERTA and other individuals discussing the possession, sale or transfer of firearms. In my experience it is common for straw purchasers of firearms to have photographs of firearms they or other individuals possess on their digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms. I also know that people keep receipts from sales and purchases of items related to firearms possession, including ammunition, holsters, etc.

23. As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the

hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital

data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.


f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the

digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

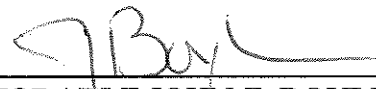
24. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

**CONCLUSION**

25. Based upon my training and experience, and the facts set forth herein, I submit that there is probable cause to believe that the items described in Attachment B are evidence of violations of Title 18, U.S.C. § 924(a)(1)(A), knowingly making a false statement or representation with respect to the information required by federal law to be kept in the records of an FFL; will be found in the **SUBJECT VEHICLE** set forth in Attachment A.

  
KATHERINE A. ROTTMAN, SPECIAL AGENT  
Bureau of Alcohol, Tobacco, Firearms &  
Explosives

Sworn to and subscribed electronically this 17th day of November 2021.

  
HONORABLE JOHN Z. BOYLE  
United States Magistrate Judge